FORMALIZED MATHEMATICS
Volume 3, Number 2, 1992
Université Catholique de Louvain

Monoids

Grzegorz Bancerek
Polish Academy of Sciences
Institute of Mathematics
Warsaw

Summary. The goal of the article is to define the concept of monoid. In the preliminary section we introduce the notion of some properties of binary operations. The second section is concerning with structures with a set and a binary operation on this set: there is introduced the notion corresponding to the notion of some properties of binary operations and there are shown some useful clusters. Next, we are concerning with the structure with a set, a binary operation on the set and with an element of the set. Such a structure is called monoid iff the operation is associative and the element is a unity of the operation. In the fourth section the concept of subsystems of monoid (group) is introduced. Subsystems are submonoids (subgroups) or other parts of monoid (group) with are closed w.r.t. the operation. The are present facts on inheritness of some properties by subsystems. Finally, there are construct the examples of groups and monoids: the group $\rangle\mathbb{R}, +\langle$ of real numbers with addition, the group $\mathbb{Z}^+$ of integers as the subsystem of the group $\rangle\mathbb{R}, +\langle$, the semigroup $\rangle\mathbb{N}, +\langle$ of natural numbers as the subsystem of $\mathbb{Z}^+$, and the monoid $\rangle\mathbb{N}, +, 0\langle$ of natural numbers with addition and zero as monoidal extension of the semigroup $\rangle\mathbb{N}, +\langle$. The semigroups of real and natural numbers with multiplication are also introduced. The monoid of finite sequences over some set with concatenation as binary operation and with empty sequence as neutral element is defined in sixth section. Last section deals with monoids with the composition of functions as the operation, i.e. with the monoid of partial and total functions and the monoid of permutations.

MML Identifier: `MONOID_0`.

The papers [15], [16], [13], [1], [6], [2], [7], [3], [5], [9], [17], [10], [14], [12], [4], [18], [8], and [11] provide the terminology and notation for this paper.

ISSN 0777–4028

1. Binary operations preliminary

In the sequel x is arbitrary and X, Y denote sets. We now define several new constructions. Let G be a 1-sorted structure. An element of G is an element of the carrier of G.

A finite sequence of elements of G is a finite sequence of elements of the carrier of G.

A binary operation on G is a binary operation on the carrier of G.

A subset of G is a subset of the carrier of G.

A 1-sorted structure is constituted functions if:

(Def.1) every element of it is a function.

A 1-sorted structure is constituted finite sequences if:

(Def.2) every element of it is a finite sequence.

Let X be a constituted functions 1-sorted structure. One can check the following observations:

* every element of X is function-like,
* every constituted finite sequences 1-sorted structure is constituted functions, and
* every constituted finite sequences half group structure is constituted functions.

Let X be a constituted finite sequences 1-sorted structure. Note that every element of X is finite sequence-like.

Let D be a non-empty set, and let p, q be finite sequences of elements of D. Then $p \frown q$ is an element of D^*. Let g, f be functions. We introduce the functor $f \circ g$ as a synonym of $f \cdot g$. Let X be a set, and let g, f be functions from X into X. Then $f \cdot g$ is a function from X into X. Let X be a set, and let g, f be permutations of X. Then $f \cdot g$ is a permutation of X. Let A be a set, and let B, C be non-empty sets, and let g be a function from A into B, and let f be a function from B into C. Then $f \cdot g$ is a function from A into C. Let A, B, C be sets, and let g be a partial function from A to B, and let f be a partial function from B to C. Then $f \cdot g$ is a partial function from A to C. Let D be a non-empty set. A binary operation on D is left invertible if:

(Def.3) for every elements a, b of D there exists an element l of D such that $\mathrm{it}(l, a) = b$.

A binary operation on D is right invertible if:

(Def.4) for every elements a, b of D there exists an element r of D such that $\mathrm{it}(a, r) = b$.

A binary operation on D is invertible if:

(Def.5) for every elements a, b of D there exist elements r, l of D such that $\mathrm{it}(a, r) = b$ and $\mathrm{it}(l, a) = b$.

A binary operation on D is left cancelable if:

(Def.6) for all elements a, b, c of D such that $\mathrm{it}(a, b) = \mathrm{it}(a, c)$ holds $b = c$.

A binary operation on D is right cancelable if:

(Def.7) for all elements a, b, c of D such that $\mathrm{it}(b, a) = \mathrm{it}(c, a)$ holds $b = c$.

A binary operation on D is cancelable if:

(Def.8) for all elements a, b, c of D such that $\mathrm{it}(a, b) = \mathrm{it}(a, c)$ or $\mathrm{it}(b, a) = \mathrm{it}(c, a)$ holds $b = c$.

A binary operation on D has uniquely decomposable unity if:

(Def.9) it has a unity and for all elements a, b of D such that $\mathrm{it}(a, b) = \mathbf{1}_{\mathrm{it}}$ holds $a = b$ and $b = \mathbf{1}_{\mathrm{it}}$.

We now state three propositions:

(1) For every non-empty set D and for every binary operation f on D holds f is invertible if and only if f is left invertible and right invertible.

(2) For every non-empty set D and for every binary operation f on D holds f is cancelable if and only if f is left cancelable and right cancelable.

(3) For every binary operation f on $\{x\}$ holds $f = \{\langle x, x\rangle\} \longmapsto x$ and f has a unity and f is commutative and f is associative and f is idempotent and f is invertible and cancelable and has uniquely decomposable unity.

2. Semigroups

We adopt the following convention: G denotes a half group structure, D denotes a non-empty set, and a, b, c, r, l denote elements of G. We now define several new attributes. A half group structure is unital if:

(Def.10) the operation of it has a unity.

A half group structure is commutative if:

(Def.11) the operation of it is commutative.

A half group structure is associative if:

(Def.12) the operation of it is associative.

A half group structure is idempotent if:

(Def.13) the operation of it is idempotent.

A half group structure is left invertible if:

(Def.14) the operation of it is left invertible.

A half group structure is right invertible if:

(Def.15) the operation of it is right invertible.

A half group structure is invertible if:

(Def.16) the operation of it is invertible.

A half group structure is left cancelable if:

(Def.17) the operation of it is left cancelable.

A half group structure is right cancelable if:

(Def.18) the operation of it is right cancelable.

A half group structure is cancelable if:

(Def.19) the operation of it is cancelable.

A half group structure has uniquely decomposable unity if:

(Def.20) the operation of it has uniquely decomposable unity.

One can verify that there exists a unital commutative associative cancelable idempotent invertible with uniquely decomposable unity constituted functions constituted finite sequences strict half group structure.

We now state a number of propositions:

(4) If G is unital, then $\mathbf{1}_{\text{the operation of } G}$ is a unity w.r.t. the operation of G.

(5) G is unital if and only if for every a holds $\mathbf{1}_{\text{the operation of } G} \cdot a = a$ and $a \cdot \mathbf{1}_{\text{the operation of } G} = a$.

(6) G is unital if and only if there exists a such that for every b holds $a \cdot b = b$ and $b \cdot a = b$.

(7) G is commutative if and only if for all a, b holds $a \cdot b = b \cdot a$.

(8) G is associative if and only if for all a, b, c holds $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(9) G is idempotent if and only if for every a holds $a \cdot a = a$.

(10) G is left invertible if and only if for every a, b there exists l such that $l \cdot a = b$.

(11) G is right invertible if and only if for every a, b there exists r such that $a \cdot r = b$.

(12) G is invertible if and only if for every a, b there exist r, l such that $a \cdot r = b$ and $l \cdot a = b$.

(13) G is left cancelable if and only if for all a, b, c such that $a \cdot b = a \cdot c$ holds $b = c$.

(14) G is right cancelable if and only if for all a, b, c such that $b \cdot a = c \cdot a$ holds $b = c$.

(15) G is cancelable if and only if for all a, b, c such that $a \cdot b = a \cdot c$ or $b \cdot a = c \cdot a$ holds $b = c$.

(16) G has uniquely decomposable unity if and only if the operation of G has a unity and for all elements a, b of G such that $a \cdot b = \mathbf{1}_{\text{the operation of } G}$ holds $a = b$ and $b = \mathbf{1}_{\text{the operation of } G}$.

(17) If G is associative, then G is invertible if and only if G is unital and the operation of G has an inverse operation.

One can check the following observations:

* every group-like half group structure is associative and invertible,
* every associative invertible half group structure is group-like,
* every half group structure which is invertible is also left invertible and right invertible,
* every half group structure which is left invertible and right invertible is also invertible,

* every cancelable half group structure is left cancelable and right cancelable,
* every left cancelable right cancelable half group structure is cancelable,
* every half group structure which is associative and invertible is also unital and cancelable,
* every Abelian group is commutative, and
* every commutative group is Abelian.

3. Monoids

We consider monoid structures which are extension of a half group structure and are systems

⟨a carrier, an operation, a unity⟩,

where the carrier is a non-empty set, the operation is a binary operation on the carrier, and the unity is an element of the carrier.

In the sequel M will be a monoid structure. A monoid structure is well unital if:

(Def.21) the unity of it is a unity w.r.t. the operation of it.

Next we state the proposition

(18) M is well unital if and only if for every element a of M holds (the unity of M) $\cdot a = a$ and $a \cdot$ the unity of $M = a$.

Let us mention that every monoid structure which is well unital is also unital.

We now state the proposition

(19) For every M being a monoid structure such that M is well unital holds the unity of $M = \mathbf{1}_{\text{the operation of } M}$.

We now define two new modes. Let us note that there exists a well unital commutative associative cancelable idempotent invertible with uniquely decomposable unity unital constituted functions constituted finite sequences strict monoid structure.

A monoid is a well unital associative monoid structure.

Let G be a half group structure. A monoid structure is called a monoidal extension of G if:

(Def.22) the half group structure of it = the half group structure of G.

One can prove the following proposition

(20) For every monoidal extension M of G holds the carrier of M = the carrier of G and the operation of M = the operation of G and for all elements a, b of M and for all elements a', b' of G such that $a = a'$ and $b = b'$ holds $a \cdot b = a' \cdot b'$.

Let G be a half group structure. Note that there exists a strict monoidal extension of G.

The following proposition is true

(21) Let G be a half group structure. Let M be a monoidal extension of G. Then if G is unital, then M is unital and also if G is commutative, then M is commutative and also if G is associative, then M is associative and also if G is invertible, then M is invertible and also if G has uniquely decomposable unity, then M has uniquely decomposable unity and also if G is cancelable, then M is cancelable.

Let G be a constituted functions half group structure. One can check that every monoidal extension of G is constituted functions.

Let G be a constituted finite sequences half group structure. Note that every monoidal extension of G is constituted finite sequences.

Let G be a unital half group structure. Observe that every monoidal extension of G is unital.

Let G be an associative half group structure. One can verify that every monoidal extension of G is associative.

Let G be a commutative half group structure. One can verify that every monoidal extension of G is commutative.

Let G be an invertible half group structure. Note that every monoidal extension of G is invertible.

Let G be a cancelable half group structure. One can check that every monoidal extension of G is cancelable.

Let G be a half group structure with uniquely decomposable unity. Note that every monoidal extension of G is with uniquely decomposable unity.

Let G be a unital half group structure. Note that there exists a well unital strict monoidal extension of G.

The following proposition is true

(22) For every G being a unital half group structure and for all well unital strict monoidal extensions M_1, M_2 of G holds $M_1 = M_2$.

4. Subsystems

We now define two new modes. Let G be a half group structure. A half group structure is said to be a subsystem of G if:

(Def.23) the operation of it $\leq$ the operation of G.

Let G be a half group structure. One can check that there exists a subsystem of G which is strict.

Let G be a unital half group structure. Observe that there exists a subsystem of G which is unital associative commutative cancelable idempotent invertible with uniquely decomposable unity and strict.

Let G be a half group structure. A monoid structure is called a monoidal subsystem of G if:

(Def.24) the operation of it $\leq$ the operation of G and for every M being a monoid structure such that $G = M$ holds the unity of it $=$ the unity of M.

Let G be a half group structure. Note that there exists a monoidal subsystem of G which is strict.

Let M be a monoid structure. Let us note that the monoidal subsystem of M can be characterized by the following (equivalent) condition:

(Def.25) the operation of it $\leq$ the operation of M and the unity of it $=$ the unity of M.

Let G be a well unital monoid structure. Observe that there exists a well unital associative commutative cancelable idempotent invertible with uniquely decomposable unity strict monoidal subsystem of G.

We now state the proposition

(23) For every G being a half group structure every monoidal subsystem of G is a subsystem of G.

Let G be a half group structure, and let M be a monoidal extension of G. We see that the subsystem of M is a subsystem of G. Let G_1 be a half group structure, and let G_2 be a subsystem of G_1. We see that the subsystem of G_2 is a subsystem of G_1. Let G_1 be a half group structure, and let G_2 be a monoidal subsystem of G_1. We see that the subsystem of G_2 is a subsystem of G_1. Let G be a half group structure, and let M be a monoidal subsystem of G. We see that the monoidal subsystem of M is a monoidal subsystem of G.

We now state the proposition

(24) G is a subsystem of G and M is a monoidal subsystem of M.

In the sequel H is a subsystem of G and N is a monoidal subsystem of G. One can prove the following propositions:

(25) The carrier of $H \subseteq$ the carrier of G and the carrier of $N \subseteq$ the carrier of G.

(26) For every G being a half group structure and for every subsystem H of G holds the operation of $H =$ (the operation of G) $\restriction$ [: the carrier of H, the carrier of H :].

(27) For all elements a, b of H and for all elements a', b' of G such that $a = a'$ and $b = b'$ holds $a \cdot b = a' \cdot b'$.

(28) For all subsystems H_1, H_2 of G such that the carrier of $H_1 =$ the carrier of H_2 holds the half group structure of $H_1 =$ the half group structure of H_2.

(29) For all monoidal subsystems H_1, H_2 of M such that the carrier of $H_1 =$ the carrier of H_2 holds the monoid structure of $H_1 =$ the monoid structure of H_2.

(30) For all subsystems H_1, H_2 of G such that the carrier of $H_1 \subseteq$ the carrier of H_2 holds H_1 is a subsystem of H_2.

(31) For all monoidal subsystems H_1, H_2 of M such that the carrier of $H_1 \subseteq$ the carrier of H_2 holds H_1 is a monoidal subsystem of H_2.

(32) If G is unital and $\mathbf{1}_{\text{the operation of } G} \in$ the carrier of H, then H is unital and $\mathbf{1}_{\text{the operation of } G} = \mathbf{1}_{\text{the operation of } H}$.

(33) For every M being a well unital monoid structure every monoidal subsystem of M is well unital.

(34) If G is commutative, then H is commutative.

(35) If G is associative, then H is associative.

(36) If G is idempotent, then H is idempotent.

(37) If G is cancelable, then H is cancelable.

(38) If $\mathbf{1}_{\text{the operation of } G} \in$ the carrier of H and G has uniquely decomposable unity, then H has uniquely decomposable unity.

(39) For every M being a well unital monoid structure with uniquely decomposable unity every monoidal subsystem of M has uniquely decomposable unity.

Let G be a constituted functions half group structure. Observe that every subsystem of G is constituted functions and every monoidal subsystem of G is constituted functions.

Let G be a constituted finite sequences half group structure. One can verify that every subsystem of G is constituted finite sequences and every monoidal subsystem of G is constituted finite sequences.

Let M be a well unital monoid structure. Note that every monoidal subsystem of M is well unital.

Let G be a commutative half group structure. Observe that every subsystem of G is commutative and every monoidal subsystem of G is commutative.

Let G be an associative half group structure. One can verify that every subsystem of G is associative and every monoidal subsystem of G is associative.

Let G be an idempotent half group structure. Observe that every subsystem of G is idempotent and every monoidal subsystem of G is idempotent.

Let G be a cancelable half group structure. Observe that every subsystem of G is cancelable and every monoidal subsystem of G is cancelable.

Let M be a well unital monoid structure with uniquely decomposable unity. Observe that every monoidal subsystem of M is with uniquely decomposable unity.

In this article we present several logical schemes. The scheme *SubStrEx1* deals with a half group structure $\mathcal{A}$ and a non-empty subset $\mathcal{B}$ of $\mathcal{A}$ and states that:

there exists a strict subsystem H of $\mathcal{A}$ such that the carrier of $H = \mathcal{B}$
provided the following condition is met:

- for all elements x, y of $\mathcal{B}$ holds $x \cdot y \in \mathcal{B}$.

The scheme *SubStrEx2* deals with a half group structure $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:

there exists a strict subsystem H of $\mathcal{A}$ such that for every element x of $\mathcal{A}$ holds $x \in$ the carrier of H if and only if $\mathcal{P}[x]$
provided the following conditions are met:

- for all elements x, y of $\mathcal{A}$ such that $\mathcal{P}[x]$ and $\mathcal{P}[y]$ holds $\mathcal{P}[x \cdot y]$,
- there exists an element x of $\mathcal{A}$ such that $\mathcal{P}[x]$.

The scheme *MonoidalSubStrEx1* concerns a monoid structure $\mathcal{A}$ and a non-empty subset $\mathcal{B}$ of $\mathcal{A}$ and states that:

there exists a strict monoidal subsystem H of $\mathcal{A}$ such that the carrier of $H = \mathcal{B}$

provided the parameters meet the following requirements:

- for all elements x, y of $\mathcal{B}$ holds $x \cdot y \in \mathcal{B}$,
- the unity of $\mathcal{A} \in \mathcal{B}$.

The scheme *MonoidalSubStrEx2* deals with a monoid structure $\mathcal{A}$, and a unary predicate $\mathcal{P}$, and states that:

there exists a strict monoidal subsystem M of $\mathcal{A}$ such that for every element x of $\mathcal{A}$ holds $x \in$ the carrier of M if and only if $\mathcal{P}[x]$

provided the following requirements are met:

- for all elements x, y of $\mathcal{A}$ such that $\mathcal{P}[x]$ and $\mathcal{P}[y]$ holds $\mathcal{P}[x \cdot y]$,
- $\mathcal{P}[$the unity of $\mathcal{A}]$.

Let us consider G, a, b. Then $a \cdot b$ is an element of G. We introduce the functor $a \otimes b$ as a synonym of $a \cdot b$.

5. The examples of monoids of numbers

The unital associative invertible commutative cancelable strict half group structure $\langle \mathbb{R}, + \rangle$ is defined by:

(Def.26) $\langle \mathbb{R}, + \rangle = \langle \mathbb{R}, +_{\mathbb{R}} \rangle$.

The following propositions are true:

(40) The carrier of $\langle \mathbb{R}, + \rangle = \mathbb{R}$ and the operation of $\langle \mathbb{R}, + \rangle = +_{\mathbb{R}}$ and for all elements a, b of $\langle \mathbb{R}, + \rangle$ and for all real numbers x, y such that $a = x$ and $b = y$ holds $a \cdot b = x + y$.

(41) x is an element of $\langle \mathbb{R}, + \rangle$ if and only if x is a real number.

(42) $\mathbf{1}_{\text{the operation of } \langle \mathbb{R}, + \rangle} = 0$.

(43) For every subsystem N of $\langle \mathbb{R}, + \rangle$ and for all elements a, b of N and for all real numbers x, y such that $a = x$ and $b = y$ holds $a \cdot b = x + y$.

(44) For every unital subsystem N of $\langle \mathbb{R}, + \rangle$ holds $\mathbf{1}_{\text{the operation of } N} = 0$.

(45) For every subsystem N of $\langle \mathbb{R}, + \rangle$ such that 0 is an element of N holds N is unital and $\mathbf{1}_{\text{the operation of } N} = 0$.

Let G be a unital half group structure. Observe that every associative invertible subsystem of G is unital cancelable and group-like.

Let us note that it makes sense to consider the following constant. Then $\mathbb{Z}^+$ is a unital invertible strict subsystem of $\langle \mathbb{R}, + \rangle$.

The following two propositions are true:

(46) For every strict subsystem G of $\langle \mathbb{R}, + \rangle$ holds $G = \mathbb{Z}^+$ if and only if the carrier of $G = \mathbb{Z}$.

(47) x is an element of $\mathbb{Z}^+$ if and only if x is an integer.

We now define three new functors. The unital strict subsystem $\langle \mathbb{N}, + \rangle$ of $\mathbb{Z}^+$ with uniquely decomposable unity is defined by:

(Def.27) the carrier of $\langle \mathbb{N}, + \rangle = \mathbb{N}$.

$\langle \mathbb{N}, +, 0 \rangle$ is a well unital strict monoidal extension of $\langle \mathbb{N}, + \rangle$.

The binary operation $+_{\mathbb{N}}$ on $\mathbb{N}$ is defined by:

(Def.28) $+_{\mathbb{N}}$ = the operation of $\langle \mathbb{N}, + \rangle$.

Next we state several propositions:

(48) x is an element of $\langle \mathbb{N}, + \rangle$ if and only if x is a natural number.

(49) $\langle \mathbb{N}, + \rangle = \langle \mathbb{N}, +_{\mathbb{N}} \rangle$.

(50) x is an element of $\langle \mathbb{N}, +, 0 \rangle$ if and only if x is a natural number.

(51) For all natural numbers n_1, n_2 and for all elements m_1, m_2 of $\langle \mathbb{N}, +, 0 \rangle$ such that $n_1 = m_1$ and $n_2 = m_2$ holds $m_1 \cdot m_2 = n_1 + n_2$.

(52) $\langle \mathbb{N}, +, 0 \rangle = \langle \mathbb{N}, +_{\mathbb{N}}, 0 \rangle$.

(53) $+_{\mathbb{N}} = +_{\mathbb{R}} \restriction [\!: \mathbb{N}, \mathbb{N} :\!]$ and $+_{\mathbb{N}} = (+_{\mathbb{Z}}) \restriction [\!: \mathbb{N}, \mathbb{N} :\!]$.

(54) 0 is a unity w.r.t. $+_{\mathbb{N}}$ and $+_{\mathbb{N}}$ has a unity and $\mathbf{1}_{+_{\mathbb{N}}} = 0$ and $+_{\mathbb{N}}$ is commutative and $+_{\mathbb{N}}$ is associative and $+_{\mathbb{N}}$ has uniquely decomposable unity.

The unital commutative associative strict half group structure $\langle \mathbb{R}, \cdot \rangle$ is defined by:

(Def.29) $\langle \mathbb{R}, \cdot \rangle = \langle \mathbb{R}, \cdot_{\mathbb{R}} \rangle$.

Next we state several propositions:

(55) The carrier of $\langle \mathbb{R}, \cdot \rangle = \mathbb{R}$ and the operation of $\langle \mathbb{R}, \cdot \rangle = \cdot_{\mathbb{R}}$ and for all elements a, b of $\langle \mathbb{R}, \cdot \rangle$ and for all real numbers x, y such that $a = x$ and $b = y$ holds $a \cdot b = x \cdot y$.

(56) x is an element of $\langle \mathbb{R}, \cdot \rangle$ if and only if x is a real number.

(57) $\mathbf{1}_{\text{the operation of } \langle \mathbb{R}, \cdot \rangle} = 1$.

(58) For every subsystem N of $\langle \mathbb{R}, \cdot \rangle$ and for all elements a, b of N and for all real numbers x, y such that $a = x$ and $b = y$ holds $a \cdot b = x \cdot y$.

(59) For every subsystem N of $\langle \mathbb{R}, \cdot \rangle$ such that 1 is an element of N holds N is unital and $\mathbf{1}_{\text{the operation of } N} = 1$.

(60) For every unital subsystem N of $\langle \mathbb{R}, \cdot \rangle$ holds $\mathbf{1}_{\text{the operation of } N} = 0$ or $\mathbf{1}_{\text{the operation of } N} = 1$.

We now define three new functors. The unital strict subsystem $\langle \mathbb{N}, \cdot \rangle$ of $\langle \mathbb{R}, \cdot \rangle$ with uniquely decomposable unity is defined by:

(Def.30) the carrier of $\langle \mathbb{N}, \cdot \rangle = \mathbb{N}$.

$\langle \mathbb{N}, \cdot, 1 \rangle$ is a well unital strict monoidal extension of $\langle \mathbb{N}, \cdot \rangle$.

The binary operation $\cdot_{\mathbb{N}}$ on $\mathbb{N}$ is defined by:

(Def.31) $\cdot_{\mathbb{N}}$ = the operation of $\langle \mathbb{N}, \cdot \rangle$.

One can prove the following propositions:

(61) $\langle \mathbb{N}, \cdot \rangle = \langle \mathbb{N}, \cdot_{\mathbb{N}} \rangle$.

(62) For all natural numbers n_1, n_2 and for all elements m_1, m_2 of $\langle \mathbb{N}, \cdot \rangle$ such that $n_1 = m_1$ and $n_2 = m_2$ holds $m_1 \cdot m_2 = n_1 \cdot n_2$.

(63) $\mathbf{1}_{\text{the operation of } \langle \mathbb{N}, \cdot \rangle} = 1$.

(64) For all natural numbers n_1, n_2 and for all elements m_1, m_2 of $\langle \mathbb{N}, \cdot, 1 \rangle$ such that $n_1 = m_1$ and $n_2 = m_2$ holds $m_1 \cdot m_2 = n_1 \cdot n_2$.

(65) $\langle \mathbb{N}, \cdot, 1 \rangle = \langle \mathbb{N}, \cdot_{\mathbb{N}}, 1 \rangle$.

(66) $\cdot_{\mathbb{N}} = \cdot_{\mathbb{R}} \restriction [\!:\mathbb{N}, \mathbb{N}:\!]$.

(67) 1 is a unity w.r.t. $\cdot_{\mathbb{N}}$ and $\cdot_{\mathbb{N}}$ has a unity and $\mathbf{1}_{\cdot_{\mathbb{N}}} = 1$ and $\cdot_{\mathbb{N}}$ is commutative and $\cdot_{\mathbb{N}}$ is associative and $\cdot_{\mathbb{N}}$ has uniquely decomposable unity.

6. The monoid of finite sequences over the set

We now define three new functors. Let D be a non-empty set. The functor $\langle D^*, ^\frown \rangle$ yielding a unital associative cancelable constituted finite sequences strict half group structure with uniquely decomposable unity is defined by:

(Def.32) the carrier of $\langle D^*, ^\frown \rangle = D^*$ and for all elements p, q of $\langle D^*, ^\frown \rangle$ holds $p \otimes q = p \mathbin{^\frown} q$.

Let us consider D. $\langle D^*, ^\frown, \varepsilon \rangle$ is a well unital strict monoidal extension of $\langle D^*, ^\frown \rangle$.

The concatenation of D yielding a binary operation on D^* is defined as follows:

(Def.33) the concatenation of $D =$ the operation of $\langle D^*, ^\frown \rangle$.

We now state several propositions:

(68) $\langle D^*, ^\frown \rangle = \langle D^*, \text{the concatenation of } D \rangle$.

(69) $\mathbf{1}_{\text{the operation of } \langle D^*, ^\frown \rangle} = \varepsilon$.

(70) The carrier of $\langle D^*, ^\frown, \varepsilon \rangle = D^*$ and the operation of $\langle D^*, ^\frown, \varepsilon \rangle =$ the concatenation of D and the unity of $\langle D^*, ^\frown, \varepsilon \rangle = \varepsilon$.

(71) For all elements a, b of $\langle D^*, ^\frown, \varepsilon \rangle$ holds $a \otimes b = a \mathbin{^\frown} b$.

(72) For every subsystem F of $\langle D^*, ^\frown \rangle$ and for all elements p, q of F holds $p \otimes q = p \mathbin{^\frown} q$.

(73) For every unital subsystem F of $\langle D^*, ^\frown \rangle$ holds $\mathbf{1}_{\text{the operation of } F} = \varepsilon$.

(74) For every subsystem F of $\langle D^*, ^\frown \rangle$ such that ε is an element of F holds F is unital and $\mathbf{1}_{\text{the operation of } F} = \varepsilon$.

(75) For all non-empty sets A, B such that $A \subseteq B$ holds $\langle A^*, ^\frown \rangle$ is a subsystem of $\langle B^*, ^\frown \rangle$.

(76) The concatenation of D has a unity and $\mathbf{1}_{\text{the concatenation of } D} = \varepsilon$ and the concatenation of D is associative.

7. Monoids of mappings

We now define three new functors. Let X be a set. The semigroup of partial functions onto X yields a unital associative constituted functions strict half group structure and is defined by:

(Def.34) the carrier of the semigroup of partial functions onto $X = X \dot{\rightarrow} X$ and for all elements f, g of the semigroup of partial functions onto X holds $f \otimes g = f \circ g$.

Let X be a set. The monoid of partial functions onto X is a well unital strict monoidal extension of the semigroup of partial functions onto X.

The composition of X yields a binary operation on $X \dot{\rightarrow} X$ and is defined as follows:

(Def.35) the composition of $X =$ the operation of the semigroup of partial functions onto X.

We now state several propositions:

(77) x is an element of the semigroup of partial functions onto X if and only if x is a partial function from X to X.

(78) $\mathbf{1}_{\text{the operation of the semigroup of partial functions onto } X} = \mathrm{id}_X$.

(79) For every subsystem F of the semigroup of partial functions onto X and for all elements f, g of F holds $f \otimes g = f \circ g$.

(80) For every subsystem F of the semigroup of partial functions onto X such that id_X is an element of F holds F is unital and $\mathbf{1}_{\text{the operation of } F} = \mathrm{id}_X$.

(81) If $Y \subseteq X$, then the semigroup of partial functions onto Y is a subsystem of the semigroup of partial functions onto X.

We now define two new functors. Let X be a set. The semigroup of functions onto X yielding a unital strict subsystem of the semigroup of partial functions onto X is defined as follows:

(Def.36) the carrier of the semigroup of functions onto $X = X^X$.

Let X be a set. The monoid of functions onto X is a well unital strict monoidal extension of the semigroup of functions onto X.

The following four propositions are true:

(82) x is an element of the semigroup of functions onto X if and only if x is a function from X into X.

(83) The operation of the semigroup of functions onto $X =$ (the composition of X) $\restriction [\!: X^X, X^X :\!]$.

(84) $\mathbf{1}_{\text{the operation of the semigroup of functions onto } X} = \mathrm{id}_X$.

(85) The carrier of the monoid of functions onto $X = X^X$ and the operation of the monoid of functions onto $X =$ (the composition of X) $\restriction [\!: X^X, X^X :\!]$ and the unity of the monoid of functions onto $X = \mathrm{id}_X$.

Let X be a set. The group of permutations onto X yields a unital invertible strict subsystem of the semigroup of functions onto X and is defined by:

(Def.37) for every element f of the semigroup of functions onto X holds $f \in$ the carrier of the group of permutations onto X if and only if f is a permutation of X.

One can prove the following three propositions:

(86) x is an element of the group of permutations onto X if and only if x is a permutation of X.

(87) $\mathbf{1}_{\text{the operation of the group of permutations onto } X} = \mathrm{id}_X$ and $1_{\text{the group of permutations onto } X} = \mathrm{id}_X$.

(88) For every element f of the group of permutations onto X holds $f^{-1} = (f\ \mathbf{qua}\ \text{a function})^{-1}$.

References

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[2] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

[3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.

[4] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[5] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[6] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[7] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[8] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.

[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.

[10] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.

[11] Dariusz Surowik. Cyclic groups and some of their properties - part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.

[12] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[13] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.

[14] Andrzej Trybulec. Semilattice operations on finite subsets. *Formalized Mathematics*, 1(**2**):369–376, 1990.

[15] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[16] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(**1**):97–105, 1990.

[17] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[18] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.

Received December 29, 1992